(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 41 23 666 A 1**

(51) Int. Cl.[5]:
G 07 C 11/00
B 60 R 25/00
// E05B 65/12

(21) Aktenzeichen: P 41 23 666.1
(22) Anmeldetag: 17. 7. 91
(43) Offenlegungstag: 9. 7. 92

DE 41 23 666 A 1

(30) Unionspriorität: (32) (33) (31)
04.01.91 US 637353

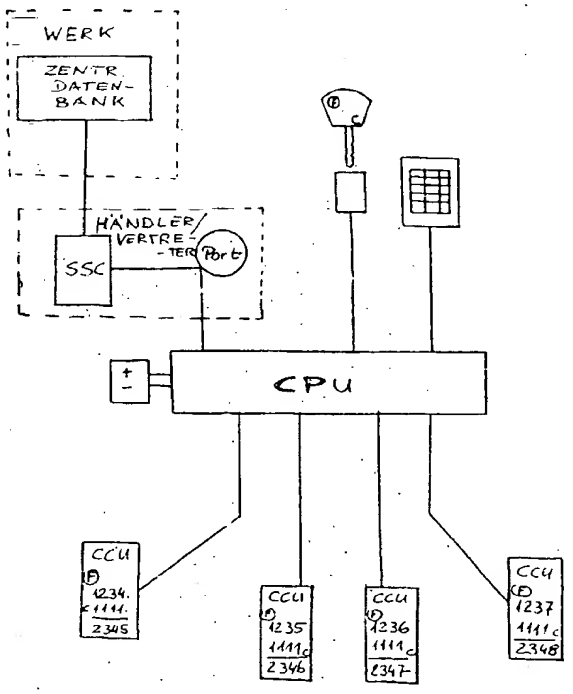
(71) Anmelder:
The Inteleplex Corp., Paramus, N.J., US

(74) Vertreter:
Müller, H., Dipl.-Ing., 8000 München; Schupfner, G., Dipl.-Chem. Dr.phil.nat., 2110 Buchholz; Gauger, H., Dipl.-Ing., Pat.-Anwälte, 8000 München

(72) Erfinder:
Sues, John M., New York, N.Y., US; Sun, Jing H., Roosevelt Island, N.Y., US

(54) Sicherheitssystem für einen mobilen Ausrüstungsgegenstand

(57) Es wird ein Sicherheitssystem für einen mobilen Ausrüstungsgegenstand wie etwa Güterwagen, Flugzeuge, Schiffe, Kraftfahrzeuge bzw. Lastwagen oder andere Maschinen, die gestohlen werden können, angegeben. Das System umfaßt eine Zentraleinheit, Mittel zum Übertragen eines Datenstroms zu verschiedenen Komponenten des Fahrzeugs und Komponentensteuereinheiten, die an jedem der Teile des geschützten Fahrzeugs befestigt sind. Die Steuereinheiten akzeptieren einen Code vom Speicher des Zündschlüssels des Fahrzeugs, ändern diesen Code und übertragen den geänderten Code zurück an die Zentraleinheit. Ferner sind Mittel vorgesehen, um bestimmte Einrichtungen, die für den Betrieb des Fahrzeugs und/oder seiner geschützten Untersysteme zuständig sind, funktionsunfähig zu machen. Diese Systeme können ihrerseits mit einer zentralen Datenbank über ein Systemsteuerzentrum verbunden sein, um den Bestand und die Regulierung von Teilen sowohl innerhalb jedes Fahrzeugs als auch zwischen sämtlichen von dem System geschützten Fahrzeugen zu steuern.



DE 41 23 666 A 1

Beschreibung

Die vorliegende Anmeldung ist eine CIP-Anmeldung der US-Patentanmeldung Serial-Nr. 3 92 092 vom 10. Aug. 1989.

Diebstahl und unerlaubte Benützung von beweglichen Ausrüstungsgegenständen wie Kraftfahrzeugen, Baumaschinen, Flugzeugen und dergleichen sind weit verbreitet. Es wurden zwar schon zahlreiche Versuche gemacht, Diebstahl und unerlaubte Benützung auf diesem Gebiet zu unterbinden, sie sind jedoch nur begrenzt erfolgreich. Es gibt daher seit langem die Nachfrage nach einem Sicherheitssystem, das derartige strafbaren Handlungen wirksam verhindert.

Die heute verfügbaren Sicherheitssysteme schrecken nicht in wirksamer Weise vom Diebstahl von Komponenten ab. Warnsysteme wie Hupen, Piepsgeräte oder Sirenen haben nur geringe Abschreckwirkung für Diebe. Insbesondere in Stadtgebieten sind Sirenen und Alarmsignale inzwischen so üblich, daß sie unwirksam sind. Funksignalsysteme sind ebenfalls unwirksam, weil sie von der Schnelligkeit und Effizienz der örtlichen Polizeireviere abhängen. Heute sind viele Polizeireviere unterbesetzt und können einen Dieb nicht fassen, bevor das Funksignalsignal unwirksam gemacht werden kann. Durch eine große Vielzahl solcher Systeme kann das Problem nur verschlimmert werden.

Es sind zwar bereits Antidiebstahlsysteme beschrieben worden, die einen elektronischen Schlüssel zum Sichern eines Kraftfahrzeugs verwenden, aber keines dieser Systeme bietet wirksamen Schutz. Ein solches Sicherheitssystem ist in der US-PS 41 92 400 beschrieben. Dort wird ein Schlüssel beschrieben, der ein Schieberegister enthält, wobei beim Einführen in das Kraftfahrzeug ein elektronischer Zeitgeber eine Wiederholung der im Schieberegister gespeicherten Informationen veranlaßt. Eine Vergleichseinrichtung vergleicht dann diese Informationen mit vorher im Fahrzeug gespeicherten Informationen. Wenn eine Übereinstimmung festgestellt wird, kann das Fahrzeug benützt werden. Wenn die Informationen aber nicht übereinstimmen, wird der Verteiler oder der Startermotor des Fahrzeugs blockiert.

Die US-PS 46 42 631 beschreibt ein interaktives Sicherheitssystem, bei dem ein erster Schaltkreis ein Kontrollsignal erzeugt und ein zweiter Schaltkreis ein Codewort liefert, das eine Folge von logischen Zuständen bezeichnet, wobei die Folge der logischen Zustände eine Funktion des Kontrollsignals ist. Ein Vergleicher vergleicht die erzeugten Signale mit einem vorbestimmten gespeicherten Signal, und bei Feststellung einer Übereinstimmung ist das Fahrzeug bzw. die sonstige Einrichtung zugänglich.

Ähnliche Sicherheitssysteme sind in den US-PS 43 00 057, 43 70 561, 43 73 242, 45 38 135, 46 72 224 und 46 76 082 beschrieben.

Die oben beschriebenen Sicherheitssysteme weisen verschiedene Nachteile auf. Beispielsweise können alle diese Sicherheitssysteme zerstört und die mobilen Gegenstände zu einem entfernten Ort transportiert, repariert und wiederverkauft werden. Oder der mobile Gegenstand kann zerlegt werden, so daß die verschiedenen Einzelteile dann gesondert verkauft werden können. Auch ist es wohlbekannt, daß Karosserieteile wie Kofferraumdeckel, Motorhauben, vordere Kotflügel sowie eigenständige Untersysteme wie Radios, Aufzeichnungsgeräte, Fernsprechtelefone oder andere elektronische Einrichtungen durch ein bestimmtes Sicherheitssystem vollkommen ungeschützt sind und somit ausgebaut und wiederverkauft werden können.

Schließlich können durch Nutzung einer zentralen Datenbank Änderungen in bezug auf die Anmeldung, den Austausch von Teilen, größere Reparaturen, Unfälle sowie das vollständige Kundendienstprotokoll eines Fahrzeugs aufgezeichnet werden. Der Zweck dieses Systems ist es, das Fahrzeug und seine Bestandteile zum Wiederverkauf durch Unbefugte wertlos und unverkäuflich zu machen. Die Datenbank enthält jedes geschützte Teil der Gesamtproduktion eines bestimmten Kraftfahrzeugmodells. Wenn ein bestimmtes geschütztes Teil wie etwa ein linker Kotflügel aus einem Fahrzeug ausgebaut und in ein anderes eingebaut wird, ist keines der Fahrzeuge betriebsfähig. Das ausgebaute Teil könnte in kein Fahrzeug der gesamten Produktionsserie eingebaut werden, so daß es für den unbefugten Benutzer wertlos ist. Dies bietet den weiteren Vorteil, daß Informationen hinsichtlich der Absatzfähigkeit und Gütesicherung gesammelt werden, die von einem Händler oder Hersteller genützt werden können. Insgesamt stellt die Erfindung nicht nur ein Sicherheitssystem bereit, sondern auch ein umfassendes System für die planmäßige Wartung eines Fahrzeugs und seiner Einzelteile sowie einen exakten Bestandsmechanismus und Vermarktungsinformationen.

Durch die Erfindung wird ein Sicherheitssystem für einen mobilen Ausrüstungsgegenstand angegeben, wobei das System aufweist: eine Komponentensteuereinheit (CCU), eine Zentraleinheit (CPU), ein Systemsteuerzentrum (SCC) und eine internationale Kontrolldatenbank (IDB). Die CCU und die CPU befinden sich dabei in dem geschützten Fahrzeug, das SCC befindet sich im Geschäft des Vertragshändlers, und die IDB befindet sich beim Hersteller, alle diese Einheiten sind jedoch für die Funktionsfähigkeit des Systems wesentlich.

Es gibt zwei Arten von Komponentensteuereinheiten bzw. CCUs:
Die erste ist passiv und einer ausgewählten Komponente eines Ausrüstungsgegenstands zugeordnet. Die CCU hat Einrichtungen zur Aufnahme und Speicherung von Daten, die während des Herstellungsprozesses eingegeben wurden, sowie von Daten von dem SCC, die durch den Vertragshändler oder die herstellerseitige Datenbank eingegeben werden können. Der Werkscode (FAC) darf während der Lebensdauer des geschützten Teils nicht geändert werden. Er kann vom SCC nicht ausgelesen werden, da er sich unter der Steuerung durch das Betriebssystem befindet, das auch die Werksdatenbank steuert. Die zweite Art ist passiv, sie hat die gleiche Speicherfähigkeit wie die passive CCU und kann außerdem die von ihr geschützten Teile funktionsunfähig machen. Die CPU empfängt Daten vom Zündschlüssel und gibt sie an die CCUs weiter, die die empfangenen Daten ändern und die geänderten Daten wieder zurück an die CPU übermitteln.

Die CPU ist in dem mobilen Ausrüstungsgegenstand angeordnet und hat Einrichtungen zum zyklischen Abfragen jeder der CCUs in der richtigen Reihenfolge sowie Einrichtungen zum Prüfen von Codes oder geänderten Codes, die von der CCU empfangen werden. Wenn Codes falsch sind oder außerhalb der richtigen Reihenfolge liegen oder fehlen, sendet die CPU eine Anweisung an die aktiven CCUs, um ihre jeweiligen Teile funktionsunfähig zu machen.

Das SCC kann Daten in den Speicher der CPU eingeben und diese Informationen mit einer zentralen Datenbank vergleichen.

Die IDB kann von dem SCC empfangene Informationen wie autorisierende Codeänderungen in dem Speicher der CPU und der CCUs korrelieren und eine Bestandsführung unterhalten. Die IDB kann sowohl den ROM- als auch den EPROM-Speicher der CCUs auslesen, während der Zugriff des SCC auf den EPROM beschränkt ist.

Die Erfindung wird nachstehend auch hinsichtlich weiterer Merkmale und Vorteile anhand der Beschreibung von Ausführungsbeispielen und unter Bezugnahme auf die beiliegenden Zeichnungen näher erläutert. Die Zeichnungen zeigen in

Fig. 1 ein Kraftfahrzeug, in das ein Kraftfahrzeugsperrteil des Systems nach der Erfindung eingebaut ist;

Fig. 2A einen elektronischen Schlüssel, der für die Anwendung der Erfindung nützlich ist;

Fig. 2B das Schlüsselerkennungs-Untersystem;

Fig. 2C einen alternativen Schlüssel mit Schlüsselerkennungs-Untersystem;

Fig. 3 die Verwendung einer Reflexionslicht-Schnittstelle zur Erkennung bewegter Teile in dem System; dabei erkennt das System das Kurbelgehäuse eines geschützten Fahrzeugs;

Fig. 4 einen Querschnitt durch die Reflexionslicht-Schnittstelle von **Fig.** 3; und

Fig. 5 ein Blockschaltbild des Sicherheitssystems nach der Erfindung.

In der folgenden Beschreibung des Sicherheitssystems wird der Ausdruck "Fahrzeug" verwendet. Dieser Ausdruck soll die Erfindung jedoch nicht auf Fahrzeuge als solche beschränken; das System ist bei allen mobilen Ausrüstungsgegenständen anwendbar.

Das Gesamtsystem umfaßt drei Hauptsysteme, die jeweils wiederum zahlreiche Untersysteme aufweisen. Die drei Hauptsysteme sind dabei:

1) das Fahrzeugsperrsystem,
2) die Händler-Geräteausrüstung und
3) die zentrale Datenbank.

Das Fahrzeugsperrsystem umfaßt eine oder mehrere Komponentensteuereinheiten (CCU) und eine Zentraleinheit (CPU), die miteinander in Verbindung stehen. Typischerweise umfaßt das System eine Vielzahl von CCUs. Davon sind einige passiv, während andere aktiv sind und an zugänglichen Stellen in einem geschützten Bauelement installiert sind. Sämtliche CCUs enthalten einen Speicher zur Speicherung von Informationen, auf die die CPU Zugriff hat. Eine Funktion der CPU ist es, Unterschriften-Codes und Folgen von codierten geschützten Teilen zu prüfen. CPU-Befehle an aktive CCUs können das Teil oder System, an dem sie angeordnet sind, sperren bzw. funktionsunfähig machen. Die CPU sendet einen solchen Befehl beispielsweise aus, wenn nach der Aufruf-Funktion einer oder mehrere Unterschriften-Codes fehlerhaft sind oder fehlen oder außerhalb der Sequenz liegen.

Das Sicherheitssystem kann bestimmen, ob geschützte Teile vom System getrennt sind. Wenn ein geschütztes Teil getrennt ist, funktioniert das Fahrzeug erst wieder, wenn die Zustimmung von der Datenbank eingetroffen ist. Wenn das geschützte Teil ungewollt getrennt wird, hat das System eine manuelle Übersteuerung, die durch einen Code über eine Tastatur im Fahrzeug, die eine vorbestimmte Anzahl von Startvorgängen zuläßt, aktivierbar ist. Dieser Vorgang ermöglicht den Betrieb des Fahrzeugs bis zur Ablieferung bei einem Vertragshändler zur Code-Auffrischung.

Die CPU steht über den Fahrzeugkabelsatz oder andere Mittel mit jeder geschützten Komponente in Verbindung. Die CPU sendet vom Zündschlüsselspeicher empfangene Information an eine CCU, die die Information ändert und sie zur CPU zurücksendet. Wenn von der CPU während der Aufrufroutine empfangene Informationen mit den im Speicher der CPU enthaltenen Informationen übereinstimmen, werden die Fahrzeugkomponenten aktiviert. (Aktivieren heißt, daß aktive Komponenten ihre Funktion für den Betrieb des Fahrzeugs aufnehmen können). Wenn an den CPU-Speicher übermittelte Informationen nicht mit den gespeicherten Informationen übereinstimmen, sendet die CPU einen Befehl an aktive CCUs, um die Komponente und das Fahrzeug zu sperren.

Die Händlerausrüstungs-Schnittstelle (DA-Schnittstelle) zwischen der Datenbank und dem Fahrzeug ist das Systemsteuerzentrum (SCC), das dem Händler gehört und von ihm betrieben wird und außerdem das Kommunikationsglied zwischen der Fahrzeug-CPU und der zentralen Datenbank darstellt. Ein Händler besitzt typischerweise eins bis fünf SCCs. Das SCC ist nicht nur das Kommunikationsglied zwischen der zentralen Datenbank und dem Fahrzeug, sondern es stellt ein wichtiges Sicherheitselement für die Integrität der Datenbank dar. Wichtige Vorgänge wie ein Wiederverkauf, eine unvorhergesehene Beschädigung, die Wartung, eine Reparatur usw. werden in der Datenbank aufgezeichnet und können von jedem autorisierten Händler überall auf der Welt abgerufen werden. SCC-Geräte ermöglichen den Ersatz von geschützten Teilen in jedem Land, in dem es Vertragshändler gibt. Zur Auswechslung eines geschützten Teils wird sein Code von der Datenbank in den CPU-Speicher eingegeben.

Der dritte wesentliche Teil des Systems ist die Internationale Datenbank (IDB), die allen Änderungen von Teilen im Fahrzeug zustimmen muß. Die IDB unterhält eine Bestandsaufnahme jedes geschützten Teils in Fahrzeugen, von Teilen, die bei Händlern auf Lager sind, und eine Werks-Bestandsaufnahme.

Die IDB verbindet in logischer Weise jedes geschützte Fahrzeug (einschließlich jeder seiner geschützten Komponenten) bestimmter Modelle und Modelljahre. Bei dem Autosafe-Sicherheitssystem wird eine Unterschriftencode-Adresse (SC-Adresse) für jede geschützte Komponente jedes weltweit hergestellten Fahrzeugs erzeugt. Infolgedessen kann für gestohlene Fahrzeuge und Komponenten, die mit dem System versehen sind, kein Wiederverkaufsmarkt entstehen. Wenn keine Autorisierung durch die zentrale Datenbank vorliegt, funktioniert ein geschütztes Teil mit dem falschen Unterschriftencode oder ohne SC nicht und läßt auch den Betrieb des Fahrzeugs, in das es eingebaut ist, nicht zu. Die IDB stellt ferner Software-Programme zur Verfügung, die zur Erhaltung der Sicherheitsintegrität des Systems erforderlich sind.

Die obige Beschreibung ist eine prinzipielle Übersicht über die Hauptsysteme bei dem System nach der Erfindung. Die drei Arten von Sperrmethoden, die in das Sicherheitssystem eingebaut werden können, werden nachstehend erläutert; dabei handelt es sich um eine aktive, eine logische und eine passive Methode.

Bei einer aktiven Sperreinrichtung werden Komponenten gesperrt bzw. unwirksam gemacht, indem ein Triac oder eine andere elektronische Schalteinrichtung in die Wicklungen eines Elektromotors, einer Lichtmaschine oder eines Relais oder in einen Spulenkörper der Wicklung eines Elektromagneten, der ein Vakuum oder

eine hydraulische Strömung steuert, eingebaut ist. "Aktiv" bezieht sich auf eine CCU, die eine Einrichtung steuert, die eine Bestätigungshandlung wie beispielsweise das Blockieren oder Sperren einer Komponente vornimmt. Baueinheiten wie das Kraftstoffeinspritzsystem und das Getriebe können durch Anwendung einer Aktivmodus-Sperrmethode geschützt werden.

Ein Beispiel für eine logische Sperrmethode ist eine an einen Prozessor, der bereits ein Bauelement wie etwa einen Verteiler steuert, übermittelte Unterbrechungsnachricht.

Passive Sperreinrichtungen arbeiten typischerweise mit einer CCU, die inaktiv wird, wenn die Komponente, an der die CCU befestigt ist, beschädigt wird. Passive Sperreinrichtungen eignen sich für Komponenten wie Stoßstangen, Kotflügel und Kofferraumdeckel. In einer passiven Sperreinrichtung ist typischerweise eine CCU in ein großes viereckiges Materialstück eingebaut, das an der geschützten Komponente befestigt ist und nicht entfernt werden kann, ohne die Elektronik der CCU zu zerstören. Beispielsweise kann die geschützte Komponente auf einer Unterlage befestigt sein, bei deren Beschädigung die CCU ein Problem anzeigt und das System blockiert. Selbst wenn der potentielle Dieb die Position der Unterlage kennt und sorgfältig darum herumschneidet, ist eine Reparatur der geschützten Komponente im Hinblick auf die Kosten nicht praktikabel.

Das System nach der Erfindung sieht Mittel vor, um Ausrüstungskomponenten zu reaktivieren, die durch Befehle von der CPU funktionsunfähig gemacht wurden. Wenn beispielsweise eine bestimmte geschützte Komponente durch eine Schalteinrichtung gesperrt ist, kann die Reaktivierung durch Befehle von der CPU erfolgen. Eine unbefugte Reparatur kann beispielsweise dadurch erschwert oder unmöglich gemacht werden, daß die geschützte Komponente in ein Gehäuse eingebracht ist, das Spezialwerkzeuge zum Öffnen benötigt. Eine andere Alternative besteht darin, eine geschützte Komponente mit einer elektronischen Schaltung zu versehen, die durch Eingabe eines speziellen digitalen Codes über eine entfernte Tastatur aktiviert oder gesperrt wird. Selbstverständlich sind auch andere Alternativen denkbar.

Service unterwegs ist in das hier angegebene System ebenfalls integrierbar. Durch Anwendung eines tragbaren Laptop-SCC und von Zelltelefonen können Service unterwegs und eine Umprogrammierung der CPU in bezug auf Ersatzteile realisiert werden. Die Anforderung von Datenbank-Änderungen durch ein tragbares SCC werden ähnlich durchgeführt, wie es für ortsfeste Einheiten beschrieben wurde, wobei als zusätzliche Vorsichtsmaßnahme Codes und verschlüsselte Sprache angewandt werden, um die Gefahr eines Abfangens der Funk- oder Kabelübertragung durch unbefugte Dritte auszuschließen. Komponenten, die durch Befehle von der CPU funktionsunfähig gemacht wurden, können durch ein tragbares oder ein ortsfestes SCC reaktiviert werden. Wenn beispielsweise eine geschützte Komponente wegen Ausfalls ausgetauscht werden muß, kann ein Ersatzteil aus dem Lager entnommen werden. Dieses Teil trägt bereits einen Werksschlüsselcode und einen Händlercode. Beide Codes sind als Ersatzteile im Gegensatz zu einem im montierten Fahrzeug befindlichen Teil erkennbar. Das Teil wird aus der Ersatzteilbestandsliste der zentralen Datenbank entfernt und in die Bestandsliste der aktiven Teile des Fahrzeugs, in das das Teil eingebaut wird, eingefügt.

Die zentrale Datenbank läßt nicht zu, daß in die Liste der aktiven Fahrzeugteile ein Teil aufgenommen wird, wenn nicht ein gleichartiges Teil aus einer Werks/Händler-Ersatzteilliste herausgenommen wird. Ebenso kann ein Teil erst dann aus der Werks/Händler-Ersatzteilliste herausgenommen werden, wenn ein fehlerhaftes gleichartiges Teil aus einer Fahrzeugteilliste herausgenommen ist. Durch Kreuzsicherung sämtlicher Teile im System ist der unbefugte Ersatz eines Teils praktisch unmöglich.

Das System nach der Erfindung weist sieben wesentliche Betriebskomponenten auf, die innerhalb der drei oben angesprochenen Hauptsysteme arbeiten:

1. Faktorkodeschlüssel, ein werkseitig installierter Code eingeprägt in den nichtflüchtigen ROM-Speicher;
2. Zündschlüssel, eine Kombination aus mechanischem Schlüssel und Werkslogik- und Benutzerlogik-Schlüssel;
3. Benutzerlogik-Schlüssel, der ein löschbarer, programmierbarer nichtflüchtiger ROM ist;
4. CPU, Systemsteuereinheit im Fahrzeug;
5. DA-Modul, Händler/Agent-Codeschlüssel und Kommunikationsbaustein im Fahrzeug mit dem SCC;
6. CCUs, die nichtflüchtigen ROM, EPROM und fakultativ Sperreinrichtung für geschützte Komponente enthalten; und
7. zentrale Datenbank, die die Identifizierung, die Lage (Fahrzeug-Zuordnung) und Archivdaten jedes geschützten Teils und Fahrzeugs aufzeichnet, schützt und speichert.

Es folgt nun die Beschreibung eines bevorzugten Ausführungsbeispiels des Sicherheitssystems.

Wenn die Stromversorgung des Fahrzeugs unterbrochen wird, wird das System gesperrt. Wenn die Stromversorgung wieder funktioniert, wird über ein Steuerungsfeld der Benutzercode eingegeben, und der Schlüssel wird in die Ein-Stellung gedreht. Das System ist dann wieder funktionsfähig.

Die erste Sequentiell-CCU ist ein elektronischer Schlüssel, der Zugangstüren öffnet und den Motor startet. Der Schlüssel hat die Funktion, die CPU zu unterbrechen, und veranlaßt die CPU, eine Codeanfrage zum Schlüssel zurückzuübertragen. Im Speicher des Zündschlüssels sind drei Schlüsselzugriffscodes gespeichert, und zwar einer vom Werk, einer vom Händler und einer vom Kunden. Das System ist insofern vielseitig, als für den Fall, daß der Händler das Fahrzeug noch nicht verkauft hat, ein spezieller Händlercode benützt werden kann, so daß das Fahrzeug eine vorbestimmte Anzahl von Malen gestartet werden kann. Wenn der Schlüssel die Nachricht von der CPU empfängt, ändert das Logikglied, das durch die drei Schlüsselcodes geändert wurde, die Nachricht und übermittelt sie wieder an die CPU. Dieser Quittungsvorgang aktiviert die CPU.

Der vom Benutzer verwendete Zündschlüssel enthält einen Speicherschlüssel (Werkscode (FAC)) und einen Kundencode (CC) sowie Leitungstreiber in seinem Griff, die mechanisch und/oder logisch Zugangstüren öffnen können. Wenn der Schlüssel im Zylinder des Zündschlosses gedreht wird, wird er aktiviert und sendet einen Unterbrechungsbefehl an die CPU.

Zum Zeitpunkt der Fertigung der geschützten Komponente wird der Werkscode auf Duplizierung geprüft und in der zentralen Datenbank gespeichert. Ein bevorzugter Code ist eine aus 16 Ziffern bestehende Codezahl

(ein sedezimaler Code).

Die Zeichnungen zeigen ein besonders bevorzugtes Ausführungsbeispiel des Systems. **Fig.** 1 zeigt verschiedene Komponenten des Systems, die in einem Kraftfahrzeug verwendet sind. Die CPU **1** empfängt den Kundencode CC vom Zündschlüsselspeicher und übermittelt die CC-Nachricht an alle geschützten Komponenten, wobei diese Nachricht wiederum von der CCU geändert wird, wenn sie das vom DAC gesteuerte Logikglied passiert, und zur CPU zur Prüfung rückübertragen wird. Die CPU fragt jede geschützte Komponente des Fahrzeugs ab, wenn der Schlüssel in seinem Zylinder gedreht wird. Die Abfrage resultiert darin, daß die CPU prüft, ob jede geschützte Komponente ordnungsgemäß dazu autorisiert ist, in dem geschützten Fahrzeug vorhanden zu sein. Wenn sämtliche geschützten Komponenten die Überprüfung bestanden haben, schaltet das System ab, bis die Abfragesequenz erneut initiiert wird.

Wenn der Benutzer Zugang zum Fahrzeug verlangt, wird ein elektrischer Zündschlüssel **2** in den Schließzylinder (nicht gezeigt) eingeführt. Durch das Einführen des Zündschlüssels fragt die CPU die geschützten Komponenten ab, die beispielsweise den Schlüssel **2**, den Schlüsselzylinder **3**, den Verteiler **4**, elektrische Einspritzer **5**, eine Kurbelwelle **6** und einen Starter **7** umfassen.

Selbstverständlich sind die hier als geschützt beschriebenen Komponenten nur Beispiele, und Komponenten in jedem bestimmten mobilen Ausrüstungsgegenstand werden vom Hersteller ausgewählt. Diese geschützten Komponenten können elektronische Systeme sowie Karosserieteile eines Kraftfahrzeugs, Stereoanlagen, Telefone, Kommunikationssysteme, Navigationsausrüstungen und dergleichen umfassen.

Das Händler-Schlüsselmodul umfaßt einen Speicher und einen Kommunikationsbaustein, der vom SCC im Geschäft des Händlers programmierbar ist. Das Händler-Schlüsselmodul kann so programmiert sein, daß es jedes bestimmte Fahrzeug betätigt und jede gewünschte Anzahl von Starts erlaubt.

Fig. 2C zeigt im einzelnen eine Art von elektronischem Schlüssel **2**, einen mechanischen Schließzylinder **3** und eine intelligente Schnittstelle. Dabei umfaßt der Schlüssel **2** einen langen Teil **10**, in dem eine Vielzahl von Elementen **11** angeordnet ist, die beim Drehen des Schlüssels elektrischen Kontakt im Aufnahmezylinder **3** herstellen sollen. Der Schließzylinder **3** enthält eine Vielzahl von Anschlußstellen **12** wie etwa einen codierten Eingang, einen ersten und einen zweiten codierten Ausgang, einen positiven Spannungsanschluß B+ und einen Masseanschluß. Selbstverständlich erkennt die CPU des Systems nach der Erfindung, ob der Schlüssel in das Zündschloß oder in eine Zugangstür eines beweglichen Ausrüstungsteils eingeführt wurde, und zwar durch Erkennung eines Steuersignals, das entweder vom ersten codierten Ausgang (Zündung) oder vom zweiten codierten Ausgang (Zugangstür) im Schließzylinder kommt. Ein solches Signal könnte beispielsweise durch geeignete logische Schaltkreise, die im Schlüssel **2** vorgesehen sind und an den codierten Eingang angelegt werden, erzeugt werden, oder es könnte durch in den Schließzylinder **3** eingebaute Schaltkreise erzeugt werden.

Geeignete mechanische und/oder elektronische Einrichtungen können aufgrund des ersten und des zweiten codierten Ausgangs Türsperren betätigen und/oder das Zündsystem des Fahrzeugs aktivieren. Solche Einrichtungen sind wohlbekannt und werden nicht näher erläutert.

Fig. 2A zeigt im einzelnen eine zweite Art von elektronischem Schlüssel **2**. Der Schlüssel hat einen langen Teil, der aus dem gleichen Material besteht und Schlüsselkerben aufweist, um Zylinderzuhaltungen wie in jedem mechanischen Schließsystem zu betätigen. Kontakte A und B sind so positioniert, daß sie mit einem Zylinder in elektrischen Kontakt gelangen, der einen seriellen Datenstrom weiterleitet, der die von der CPU ausgesandten und empfangenen codierten Nachrichten enthält.

Der Schlüssel von **Fig.** 2A wird nach dem Einführen durch Drehen um 50° im Uhrzeigersinn betätigt. Dadurch gelangt der Schlüssel mit zwei Leitern in Kontakt, die in einer Reihe mit dem Schließzylinder angeordnet sind, so daß die CPU den Speicher im Schlüssel abfragen kann. Der lange Teil des Zündschlüssels ist ein mechanischer Schlüssel, der weitere Schlösser im Fahrzeug betätigen kann.

Fig. 2B zeigt einen modifizierten Schließzylinder, der die CPU mit einem Schlüssel der in **Fig.** 2A gezeigten Art verbindet. Dabei wird ein bestehender Schließzylinder verwendet und die Schlüsselkappe modifiziert, so daß die Kontakte A und B am Schlüssel **2** über den modifizierten Zylinder elektrisch mit der CPU verbunden werden. Wie gezeigt, ist das Zylindergehäuse durch Hinzufügen eines Netzleiters von der CPU und eines Masseleiters modifiziert. Weitere Modifikationen umfassen eine Schleifringständerbefestigung und einen zusätzlichen Schleifringständer sowie einen zusätzlichen Schleifringschieber, die die Ausrichtung der Kontakte am Schlüssel und am Gehäuse gewährleisten.

Fig. 3 zeigt eine Fahrzeugkurbelwelle, die permanent mit einem optisch reflexionsfähigen Material **19** codiert ist. Diese Figur zeigt zwar das optisch reflexionsfähige Material an der Kurbelwelle, aber das System ist an jedes bewegliche Teil anpaßbar. Diese Komponente wird von der CPU mit einem Befehl an die Steuereinheit **21** (**Fig.** 4) geprüft, die Lichtstrahlen **14**, **16** erzeugt, die den codierten reflexionsfähigen Streifen **19** beleuchten.

Der reflexionsfähige Codierstreifen **19** der Kurbelwelle ändert den an die CPU zurückgeleiteten Code über eine lichtempfindliche Leseeinrichtung **20**. Wenn die CPU den geänderten Code erkennt, prüft sie, ob die Kurbelwelle zu dem Fahrzeug gehört. Elemente **15** und **17** sind ein optischer Sender bzw. ein optischer Empfänger, während die Komponente **18** ein Rahmen ist, der die verschiedenen optischen Elemente stabilisiert. Selbstverständlich ist dieses Ausführungsbeispiel mit Lichtreflexion ein Kommunikationszwischenglied, und weitere Zwischenglieder zur Übertragung von Informationen zwischen bewegten Teilen können in dem System vorgesehen sein.

Fig. 5 ist ein Blockschaltbild, das die Beziehungen zwischen den verschiedenen Komponenten des Systems nach der Erfindung verdeutlicht. F in einem Kreis bezeichnet dabei den Werkscode, während C den Kundencode bezeichnet. Die CPU empfängt die CC-Daten vom Zündschlüssel und sendet die CC-Daten an jede Komponente, die dann den Code nach Maßgabe der im DAC enthaltenen Instruktionen ändert und ein Antwortsignal aussendet, das diese Änderung reflektiert. Die CPU ist so programmiert, daß sie ein richtiges von der CCU empfangenes Signal erkennt. **Fig.** 5 zeigt ein Ausführungsbeispiel, bei dem die CCU eine einfache mathematische Manipulation des Codes durchführt, d. h. eine Addition des Kundencodes und des Werkscodes. Die CPU ist so programmiert, daß das Fahrzeug betriebsbereit ist, wenn die richtigen Sequenzen von den CCUs über-

mittelt werden.

Patentansprüche

1. Sicherheitssystem für einen mobilen Ausrüstungsgegenstand, **gekennzeichnet durch**
   a) eine Komponentensteuereinheit, die einer ausgewählten Komponente des Ausrüstungsgegenstands zugeordnet ist und Mittel aufweist zum Empfang eines Codes von einer Zentraleinheit, zum Ändern des Codes und zum Rücksenden des geänderten Codes zu der Zentraleinheit; und
   b) eine innerhalb des Ausrüstungsgegenstands angeordnete Zentraleinheit, die Mittel zum Übertragen eines Codes an die Komponentensteuereinheit und Mittel zum Prüfen des von der Komponentensteuereinheit empfangenen geänderten Codes aufweist.
2. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet, daß die Komponentensteuereinheit ferner Mittel aufweist, um die Komponente, der sie zugeordnet ist, funktionsunfähig zu machen.
3. Sicherheitssystem nach Anspruch 2, dadurch gekennzeichnet, daß die Zentraleinheit ferner Mittel aufweist, um die Komponentensteuereinheit zu veranlassen, die Komponente, der sie zugeordnet ist, funktionsunfähig zu machen.
4. Sicherheitssystem nach Anspruch 1, gekennzeichnet durch ein Systemsteuerzentrum, das die Zentraleinheit programmieren kann.
5. Sicherheitssystem nach Anspruch 4, dadurch gekennzeichnet, daß das Systemsteuerzentrum einen neuen Code in die Zentraleinheit eingeben kann.
6. Sicherheitssystem nach Anspruch 4, dadurch gekennzeichnet, daß das Systemsteuerzentrum Informationen zu einer zentralen Datenbank senden und von dort Informationen empfangen kann.
7. Sicherheitssystem nach Anspruch 6, gekennzeichnet durch eine zentrale Datenbank, die vom Systemsteuerzentrum empfangene Informationen korrelieren sowie eine Bestandsaufnahme von Informationen, die vom Systemsteuerzentrum geliefert werden, unterhalten und schützen kann.

Hierzu 4 Seite(n) Zeichnungen

Nummer: DE 41 23 666 A1
Int. Cl.[5]: G 07 C 11/00
Offenlegungstag: 9. Juli 1992

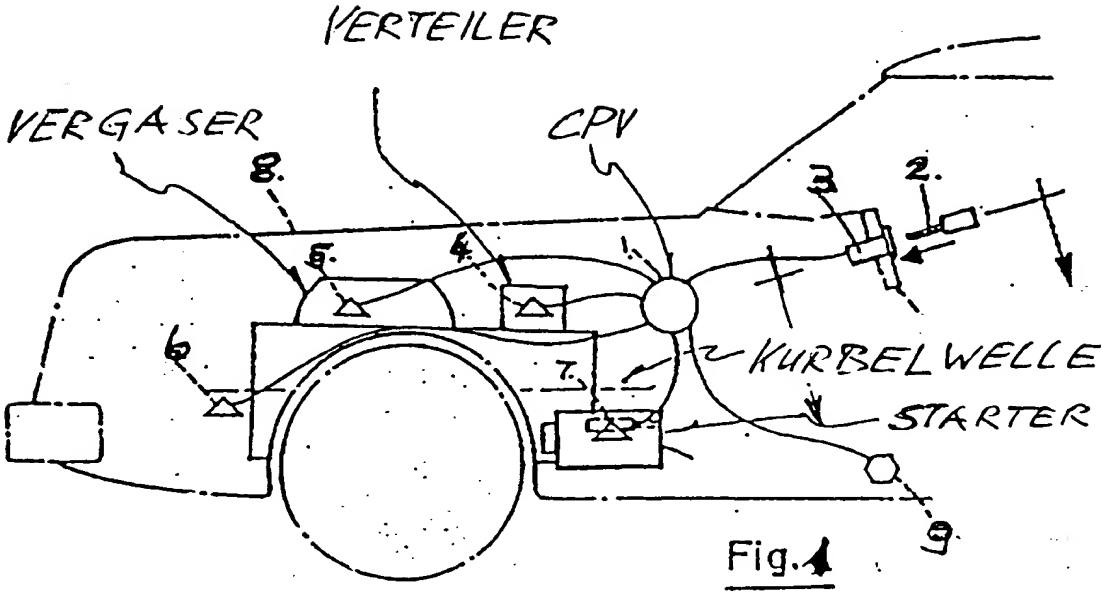


Fig. 1

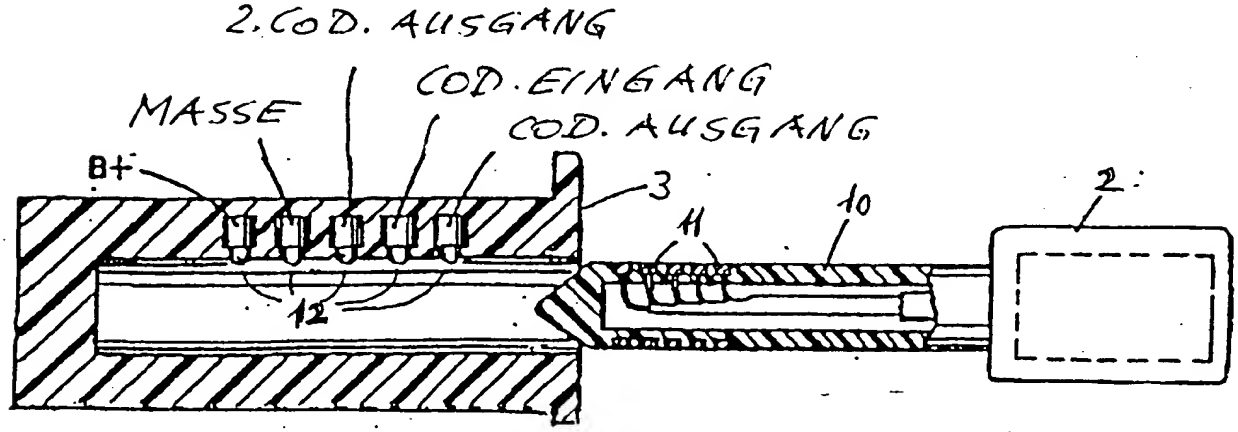


FIG 2C

Nummer: DE 41 23 666 A1
Int. Cl.[5]: G 07 C 11/00
Offenlegungstag: 9. Juli 1992

FIG 2B

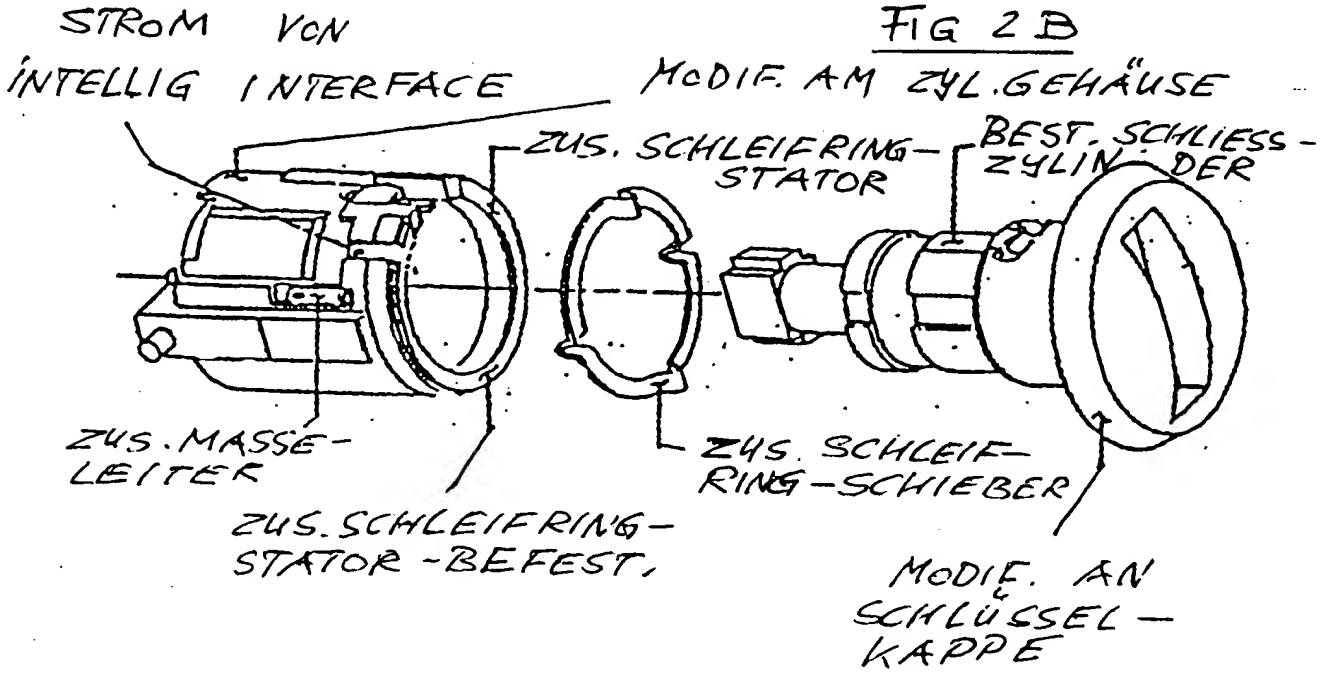
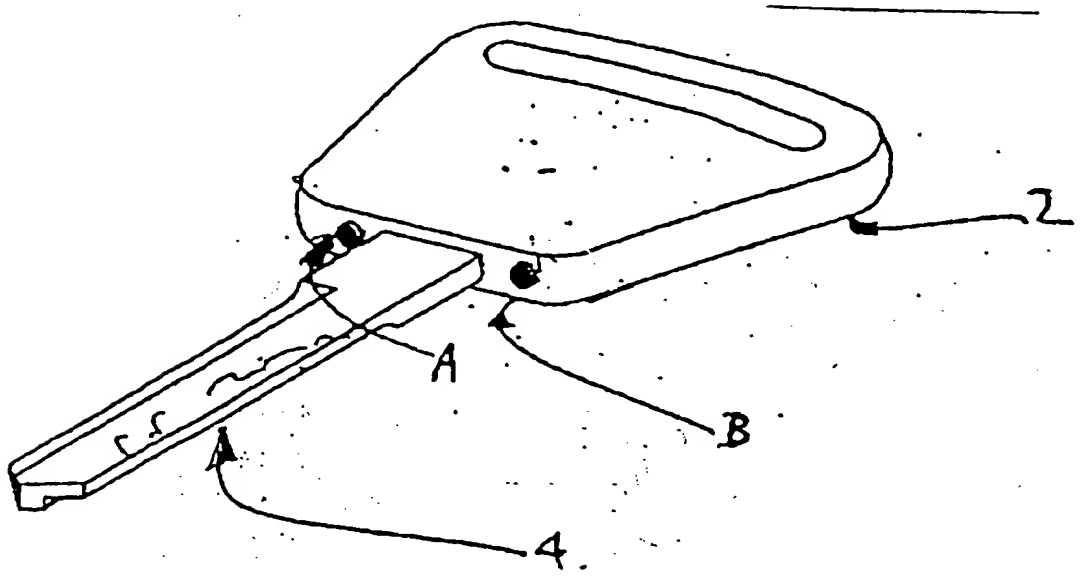


FIG. 2A



Nummer: DE 41 23 666 A1
Int. Cl.[5]: G 07 C 11/00
Offenlegungstag: 9. Juli 1992

FIG. 3

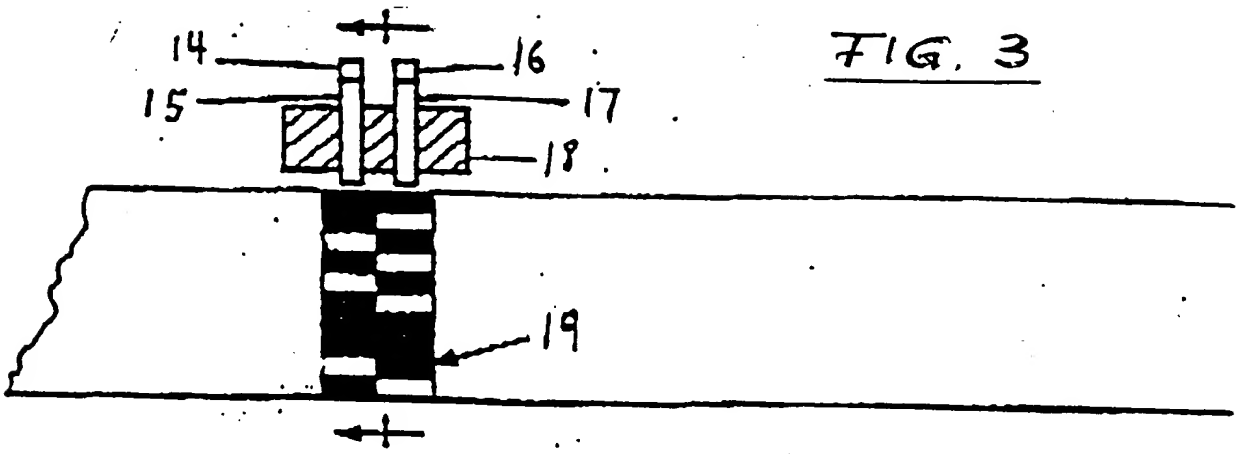
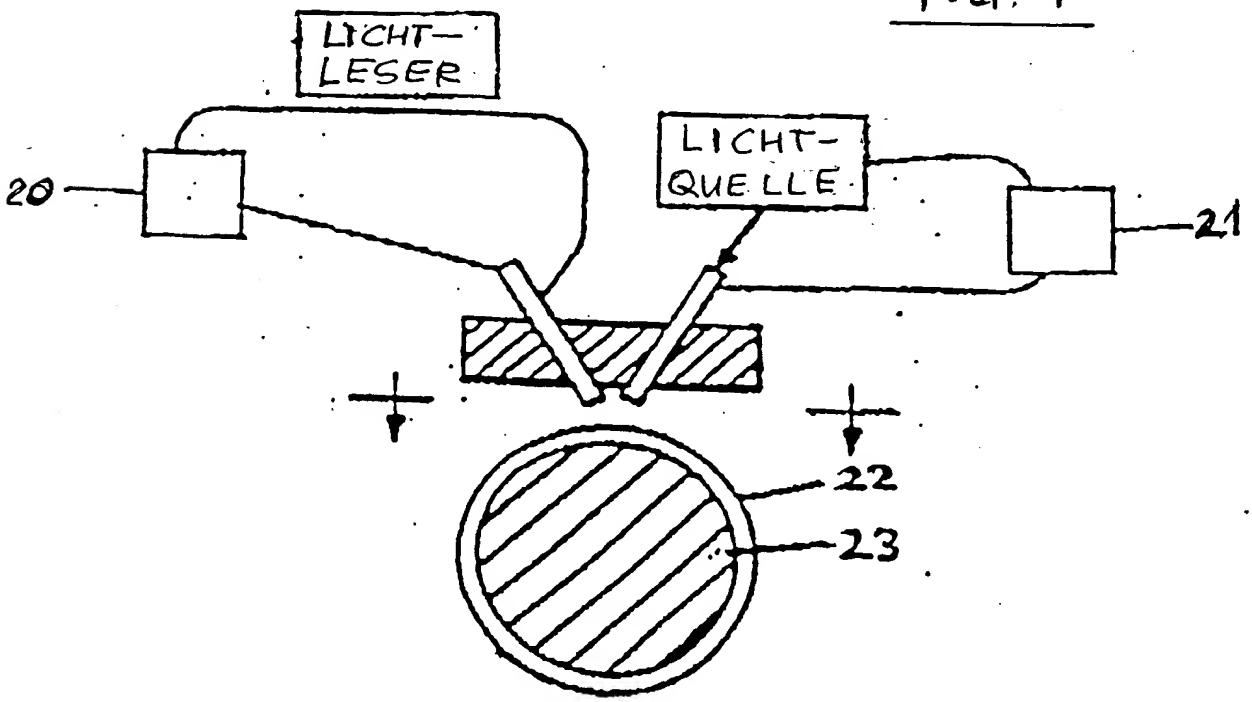


FIG. 4



Nummer: DE 41 23 696 A1
Int. Cl.[5]: G 07 C 11/00
Offenlegungstag: 9. Juli 1992

FIG. 5